UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

ENIGMA SOFTWARE GROUP USA, LLC,

Plaintiff,

v.

MALWAREBYTES INC.,

Defendant.

Case No. 1:16-cv-07885 (PAE)

MALWAREBYTES INC.'S MEMORANDUM OF LAW IN SUPPORT OF ITS MOTION TO DISMISS FIRST AMENDED COMPLAINT PURSUANT TO FEDERAL RULES OF CIVIL PROCEDURE 12(b)(2) AND 12(b)(6) AND ALTERNATIVE MOTION TO TRANSFER PURSUANT TO 28 U.S.C. § 1404

TABLE OF CONTENTS

Page

TABLE OF CONTENTS
(Continued)

Page

TABLE OF AUTHORITIES

Page(s)

CASES

TABLE OF AUTHORITIES
(Continued)

Page(s)

TABLE OF AUTHORITIES
(Continued)

Page(s)

STATUTES

OTHER AUTHORITIES

INTRODUCTION

Through this lawsuit, Plaintiff Enigma Software Group USA, LLC ("Enigma" or "Plaintiff") seeks to prevent Malwarebytes Inc. ("Malwarebytes") from distributing software that helps protect its customers from deceptive computer programs like Enigma's. Malwarebytes is a respected developer of Internet security software, and provides security software used by both consumers and enterprises to block and remove malicious software, as well as deceptive potentially unwanted programs known as "PUPs." Like other providers of security software, Malwarebytes relies on statutory protections under the Good Samaritan provision of the Communications Decency Act of 1996 ("CDA"), 47 U.S.C. § 230(c)(2), that Congress created to encourage the development of technologies designed to filter objectionable content. Absent such protection, legitimate security software vendors would be under constant threat of suits from distributors of deceptive and harmful software, ultimately discouraging the distribution of security software designed to protect consumers. That is not the result Congress envisioned when it created the Good Samaritan provision of the CDA, and it should not be the result here.

Like most Internet security software developers, Malwarebytes periodically updates its criteria for identifying malware and PUPs, making a recent update to its PUP criteria on October 5, 2016. Enigma's SpyHunter and RegHunter programs were among several other programs that qualified as PUPs under the updated criteria, and Malwarebytes began identifying those programs as "non-malware" "potentially unwanted programs" when detected on its users' computers. Among other reasons for being labeled a PUP, Enigma uses deceptive scare tactics, warning users of its free "scanner" that standard files like web browser cookies are "infections" and "spyware" and then requiring them to purchase a subscription to remove them. These tactics capitalize on consumers' fear about "spyware" to trick them into entering costly subscription plans. In keeping with its long history of threatening or engaging legal action to quash any

exposé of its practices, Enigma filed this suit. After Malwarebytes first moved to dismiss Enigma's original complaint, Enigma filed a First Amended Complaint ("FAC").

The FAC does not cure the deficiencies of the original complaint. As a threshold matter, this action should be transferred to the Northern District of California pursuant to 28 U.S.C. § 1404. Neither the parties nor the underlying facts of this case have a meaningful connection to New York, and nearly all of the witnesses and evidence are in the Northern District of California. Second, this Court lacks personal jurisdiction over Malwarebytes, which is not a New York citizen and lacks sufficient contacts with New York. Third, even if jurisdiction and venue were proper, the FAC fails to state facts sufficient to establish its claims.

Plaintiff cannot state a claim because Malwarebytes is immune from suit under the Good Samaritan provision of the CDA. *See*, *e.g.*, *Zango, Inc. v. Kaspersky Lab, Inc.*, 568 F.3d 1169, 1170 (9th Cir. 2009) (holding that a "distributor of Internet security software is entitled to immunity under the safe harbor provision of the [CDA] from a suit claiming that its software interfered with the use of downloadable programs"). Malwarebytes' software's identification of PUPs like SpyHunter and RegHunter is precisely the type of activity Section 230 immunizes.

Aside from failing to pierce that immunity, Enigma also fails to state claims of false advertising, unfair competition, or tortious interference. Consumers ultimately decide whether to use Enigma's programs in response to Malwarebytes' opinion that programs are *potentially* unwanted. FAC ¶¶ 84, 86, 93. Users can keep the program by selecting a conspicuous "Restore" button, and they must take an affirmative step to delete the program. *Id.* Thus, on the face of the FAC, Malwarebytes does not prevent consumers from using Enigma's software. The reality that not all consumers want to use or keep using Enigma's software is not grounds for Enigma's claims against Malwarebytes.

BACKGROUND

A. Malwarebytes Identifies Potentially Unwanted Programs for Its Customers.

Malwarebytes offers anti-malware and security software designed to protect consumers' computers from malware, including viruses, trojans and adware. FAC ¶ 3; Declaration of Mark Harris in Support of Malwarebytes' Motion to Dismiss ("Harris Decl.") ¶ 2. For consumers who have chosen to install it, Malwarebytes' software detects malware and PUPs on users' computers. FAC ¶¶ 4–5, 55. Malwarebytes identifies and categorizes non-malware such as PUPs differently to users, who can choose to remove the PUPs after reviewing them. *See id*. ¶¶ 5, 82, 84, 86. Malwarebytes recently acquired a standalone program, AdwCleaner, which detects adware, unwanted toolbars, and PUPs on users' computers. *Id.* ¶ 12, Exs. 2, 10.

Developers of PUPs often mask the unwanted nature of programs by including legitimate software characteristics. *See id*., Exs. 1, 12. As an ongoing and continuous effort, Malwarebytes considers many criteria and necessarily updates those criteria as developers change their programs to circumvent Malwarebytes' detection. *Id.* In October 2016, as on many previous occasions to protect users, Malwarebytes revised and published its criteria for identifying PUPs. *Id*. ¶¶ 7, 29, 73, Exs. 1, 4, 12 (revised criteria).

Malwarebytes' updated PUP criteria consider whether a program or its developer engages in: (1) obtrusive, misleading, or deceptive advertising, branding, or search practices; (2) excessive or deceptive distribution, affiliate or opt-out bundling practices; (3) aggressive or deceptive behavior especially surrounding purchasing or licensing; (4) unwarranted, unnecessary, excessive, illegitimate, or deceptive modifications of system settings or configuration (including browser settings and toolbars); (5) difficulty uninstalling or removing the software; (6) diminished user experience; and (7) other practices generally accepted as riskware, scareware, adware, greyware, or otherwise commonly unwanted software by the user community. FAC ¶ 73, Ex. 12. To

illustrate, a program may be a PUP if it uses scare tactics or misleading alerts that compel users to purchase software or upgrades with the mistaken belief that doing so is necessary to secure their computers. Malwarebytes may also identify programs that a user unintentionally installs, such as through bundled software, or that are difficult to uninstall. *See id.*

Malwarebytes considers actual harm to consumers by reviewing whether users have predominantly given program negative feedback. *Id.*; *see also* FAC ¶ 29, Ex. 4. Indeed, many users voiced their approval of Malwarebytes' updated PUP criteria and even requested greater protection from PUPs. *See* FAC, Ex. 1 at 2 (commenting that PUPs are "more insidious" than known "nefarious programs"), Ex. 6 at 4 ("PUP's [sic] are malware by every definition").

Enigma's SpyHunter and RegHunter qualify as PUPs under Malwarebytes' revised criteria, and on October 5, 2016, Malwarebytes' software began detecting those programs. FAC ¶¶ 7, 9. Significant negative feedback from consumers about Enigma's programs and Malwarebytes' own assessment showed that, among other deceptive behavior, Enigma's programs aggressively—and deceptively—identify standard web browser cookies as "infections" and "spyware" in order to scare users into making purchases and stymie users from uninstalling the programs. *Id*. ¶¶ 48–49, Exs. 1, 12; Request for Judicial Notice ("RJN"), Exs. 1–3.

Ultimately the Malwarebytes user decides whether a PUP—including SpyHunter or RegHunter—is actually unwanted and whether to keep it. When those programs are installed or are attempting to be installed on the computer of a Malwarebytes user, Malwarebytes' software identifies the programs as "non-malware" "potentially unwanted program[s]." FAC ¶¶ 86, 93 (screenshots showing the alerts to a "potentially unwanted program" and giving the option to "restore" or "delete" it); *see also id.* ¶ 32 (screenshot of AdwCleaner's detection of SpyHunter showing prompt to the user to "[p]lease uncheck elements you want to keep"). The user must

affirmatively choose restoration or deletion of PUPs. *See id.* If the user values the SpyHunter or RegHunter programs installed on the computer and wants to continue using them, the user may "restore" the programs and exclude them from Malwarebytes' detection. FAC ¶¶ 88, 90.

B. Malwarebytes Lacks Significant Contacts With New York.

Malwarebytes is a Delaware corporation with its principal place of business in Santa Clara, California, where the majority of its employees and business records are based. FAC ¶ 36; Harris Decl. ¶ 4, Ex. A. Malwarebytes does not maintain an office or data center in New York. Harris Decl. ¶ 5. Nor has it availed itself of New York law through its software licenses and customer agreements, which state that California law governs them and that all court actions arising from them shall be in California. *See id*. ¶ 7, Ex. B.

Malwarebytes offers free and purchasable versions[1] of its security software to individual users through its website, www.malwarebytes.com. *Id.* ¶ 6. This website is not specific to any state or geography; it is generally accessible to any Internet user who can navigate to it. *Id*. Users can download and install the free software without ever disclosing where they reside. *Id.*

Separate from its consumer software, Malwarebytes sells anti-malware and security software for enterprise use. Harris Decl. ¶ 2. These sales occur through Malwarebytes' website or through sales personnel, some of whom work remotely. *Id.* ¶ 8. Although five sales employees work remotely from their homes in New York, none of them has had any role in developing or updating Malwarebytes' PUP criteria. *Id.* ¶ 10; FAC ¶ 37, Ex. 8. Malwarebytes' web pages for its consumer and business products do not mention New York. Harris Decl. ¶ 11, Ex. C.

C. None of the Parties, Known Witnesses, or Evidence Are in New York.

Neither Enigma nor the conduct it alleges has any meaningful connection to New York.

[1] In addition to detecting and allowing removal of malware and PUPs, the purchasable Malwarebytes Anti-Malware Premium Software blocks malicious websites, and offers real-time malware detection, faster scanning, and scheduled scans and updates. Harris Decl. ¶¶ 2, 3.

Enigma is a Florida LLC with its principal place of business in Florida. FAC ¶ 35. The Malwarebytes activity giving rise to Plaintiff's claims is also outside New York. The core issue of each of Plaintiff's four claims is Malwarebytes' classification of Enigma's software as potentially unwanted, as well as the reason for revising the criteria for PUP classification. *See, e.g.*, *id.* ¶¶ 142, 147, 157, 167. None of these activities took place in New York. Malwarebytes employs a team of researchers who develop, refine, and execute the PUP criteria, which must be updated frequently to keep up with the dynamic and quickly changing nature of computer security. Harris Decl. ¶ 13. Members of that team, who could testify about the criteria, are based in Malwarebytes' California headquarters or work remotely outside the United States. *Id*. ¶ 16.

D. Malwarebytes and Bleeping Computer Have Minimal Contacts.

Enigma pleads that its lawsuit against Bleeping Computer LLC ("Bleeping") in this District[2] prompted Malwarebytes' decision to revise its PUP criteria. FAC ¶¶ 21, 76. As the Court is aware, Enigma sued Bleeping for libel and unfair advertising based on a Bleeping user's review of SpyHunter. Bleeping is not a software producer like Malwarebytes, but instead is the operator of a website "for computer users to learn how to use and receive support for their computer and a place 'for the novice user to learn basic concepts about Computer Technology.'" *Bleeping Computer*, Dkt. 25 ¶ 2. Bleeping is one of many participants in an affiliate program run by a third-party independent contractor, Cleverbridge, on behalf of Malwarebytes. Harris Decl. ¶ 18. Like other similar affiliates, Bleeping receives a small commission when people click on a Malwarebytes link and subsequently make a download or purchase. Those purchases amount to an immaterial amount of revenue for Malwarebytes. *Id*. Enigma's claims in the separate *Bleeping*

[2] *Enigma Software Grp. USA, LLC v. Bleeping Cmptr. LLC*, 16-00057 ("*Bleeping Computer*").

Computer case are based on Bleeping's conduct and are wholly distinct from the claims and issues in Enigma's case against Malwarebytes.

ARGUMENT

I. LEGAL STANDARDS

A. Transfer Under 28 U.S.C. § 1404 to a More Convenient Venue.

When evaluating a motion to transfer under 28 U.S.C. § 1404, the court first considers "whether the action could have been brought in the transferee district." *Everlast World's Boxing Headquarters Corp. v. Ringside, Inc.*, 928 F. Supp. 2d 735, 743 (S.D.N.Y. 2013) (citations omitted).[3] If so, the court has discretion to transfer the matter to a more convenient forum. That discretion is guided by a number of factors:

> (1) the convenience of the witnesses; (2) the convenience of the parties; (3) the location of relevant documents and the relative ease of access to sources of proof; (4) the locus of operative facts; (5) the availability of process to compel the attendance of unwilling witnesses; (6) the relative means of the parties; (7) the forum's familiarity with the governing law; (8) the weight accorded the plaintiff's choice of forum; and (9) trial efficiency and the interests of justice.

Id. (citations omitted). On a motion to transfer venue, the court may consider the defendant's "factual submissions, including declarations" that are outside of the pleadings. *Id.* at 737.

B. Dismissal Under Rule 12(b)(2) for Lack of Personal Jurisdiction.

Federal Rule of Civil Procedure 12(b)(2) requires dismissal where a plaintiff fails to carry its burden of showing the court has personal jurisdiction over the defendant. *Rates Tech., Inc. v. Cequel Commc'ns, LLC*, 15 F. Supp. 3d 409, 414 (S.D.N.Y. 2014). To defeat a Rule 12(b)(2) motion, a plaintiff must "'plead[] in good faith, legally sufficient allegations of jurisdiction,' i.e., by making a '*prima facie* showing' of jurisdiction." *Jazini v. Nissan Motor Co., Ltd.*, 148 F.3d

[3] This Court has previously noted that it may "address venue applications at the threshold, 'when there is a sound prudential justification for doing so,' because 'neither personal jurisdiction nor venue is fundamentally preliminary in the sense that subject-matter jurisdiction is.'" *Cavit Cantina Viticoltori Consorzio Cantine Sociali Del Trentino Societa' Cooperativa v. Browman Family Vineyards, Inc.*, 656 F. Supp. 2d 421, 424 (S.D.N.Y. 2009) (quoting *Leroy v. Great W. United Corp.*, 443 U.S. 173, 180 (1979)).

181, 184 (2d Cir. 1998) (internal citations omitted). Courts engage in a two-step inquiry to determine whether personal jurisdiction over a defendant exists. *DH Servs., LLC v. Positive Impact, Inc.*, No. 12-6153, 2014 WL 496875, at *2 (S.D.N.Y. Feb. 5, 2014).

The Court must first distinguish between general and specific jurisdiction. *DH Servs.*, 2014 WL 496875, at *3 (citing *Daimler AG v. Bauman*, 134 S. Ct. 746, 751 (2014)). A defendant is subject to general jurisdiction when its contacts are "so constant and pervasive 'as to render [it] essentially at home in the forum State.'" *Daimler*, 134 S. Ct. at 751 (citing *Goodyear Dunlop Tires Operations, S.A. v. Brown*, 131 S. Ct. 2846, 2851 (2011)). Absent exceptional circumstances, a corporation is not subject to general jurisdiction outside its place of incorporation or principal place of business. *See id.* at 760 (citation omitted).

For specific jurisdiction, in "'a federal question case where [the] defendant resides outside the forum state . . . the Court applies 'the forum state's personal jurisdiction rules.'" *DH Servs.*, 2014 WL 496875, at *2 (quoting *Marvel Characters, Inc. v. Kirby*, 726 F.3d 119, 128 (2d Cir. 2013)); *see also Daimler*, 134 S. Ct. at 753. New York's long-arm statute provides that a New York court may extend personal jurisdiction over any non-resident person who:

> 1. transacts any business within the state or contracts anywhere to supply goods or services in the state; or 2. commits a tortious act within the state[;] . . . or 3. commits a tortious act without the state causing injury to person or property within the state . . . if he (i) regularly does or solicits business, or engages in any other persistent course of conduct, or derives substantial revenue from goods used or consumed or services rendered, in the state, or (ii) expects or should reasonably expect the act to have consequences in the state and derives substantial revenue from interstate or international commerce . . . .

CPLR § 302(a)).

Second, the court must consider whether its exercise of personal jurisdiction comports with Due Process under the United States Constitution. *Sonera Holding B.V. v. Çukurova Holding A.Ş.*, 750 F.3d 221, 224 (2d Cir. 2014) (per curiam), *cert. denied*, 134 S. Ct. 2888,

(2014). Thus, even if a defendant's acts were within the scope of CPLR § 302, the court must determine whether the out-of-state defendant has "minimum contacts" with the forum state such that the exercise of jurisdiction does not offend "'traditional notions of fair play and substantial justice.'" *Int'l Shoe Co. v. Washington*, 326 U.S. 310, 316 (1945).

When evaluating a motion to dismiss under Rule 12(b)(2), a court may consider declarations and materials outside of the pleading. *Everlast*, 928 F. Supp. 2d at 737 (citations omitted). A court may "not draw 'argumentative inferences' in the plaintiff's favor." *Licci v. Lebanese Canadian Bank, SAL*, 673 F.3d 50, 59 (2d Cir. 2012) (internal citations omitted). If a defendant "rebuts [a plaintiff's] unsupported allegations with direct highly specific, testimonial evidence regarding a fact essential to jurisdiction—and plaintiff[] do[es] not counter that evidence—the allegation may be deemed refuted." *MEE Direct, LLC v. Tran Source Logistics, Inc.*, No. 12-6916, 2012 WL 6700067, at *2 (S.D.N.Y. Dec. 26, 2012) (citation, internal quotation marks, and footnote omitted).

C. Dismissal Under Rule 12(b)(6) for Failure to State a Claim.

To survive a motion to dismiss under Rule 12(b)(6), a complaint must plead "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). A claim will only have "facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). A complaint is properly dismissed, where, as a matter of law, "the allegations in a complaint, however true, could not raise a claim of entitlement to relief." *Twombly*, 550 U.S. at 558. Although the court must accept all of a complaint's allegations as true when considering a motion to dismiss, this tenet does not apply to legal conclusions. *Twombly*, 550 U.S. at 555. "Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." *Iqbal*, 556 U.S. at 678.

II. THE SECTION 1404 FACTORS STRONGLY FAVOR TRANSFERRING THIS CASE TO THE NORTHERN DISTRICT OF CALIFORNIA

A. This Case Could Have Been Brought in the Northern District of California.

The Northern District of California would have both subject matter and personal jurisdiction over this case. *See, e.g.*, 28 U.S.C. §§ 1331, 1332, 1367. That district's basis for subject matter jurisdiction would be no different from this Court's. And because Malwarebytes has its principal place of business in the Northern District of California, personal jurisdiction and venue are both proper there. Harris Decl. ¶ 4; *see* § 1391(b), (c).

B. The Section 1404 Factors Favor Transfer.

1. The Convenience of Witnesses Favors Transfer.

As this Court has previously recognized, "[t]he convenience of witnesses is an important consideration, and has often been described as the single most important § 1404(a) factor." *Everlast*, 928 F. Supp. 2d at 743 (citations omitted) (granting motion to transfer in case asserting breach of contract and Lanham Act claims where the defendants and operative events lacked a connection to New York). Transfer is favored where, as here, witnesses are "dominantly sited" in the transferee district and the defendants' employees and former employees would be called to testify. *See SBAV LP v. Porter Bancorp, Inc.*, No. 13-372, 2013 WL 3467030, at *7 (S.D.N.Y. July 10, 2013). In *SBAV*, the court noted that "the long-distance travel required [of employee witnesses] could impede trial in this district and would impose substantial expense on witnesses or the parties calling them." *Id.* at *8 (citation omitted).

The most relevant witnesses are Malwarebytes employees who will testify to the central factual dispute critical to each of Plaintiff's four claims: Malwarebytes' reason for revising its PUP criteria, causing Enigma's products to be classified as PUPs. None of these witnesses is in New York; most are in California. Harris Decl. ¶¶ 10, 16. Also, to refute Enigma's allegation

that Malwarebytes is a direct competitor trying to unfairly undermine its business, FAC ¶¶ 4, 54, Malwarebytes expects to offer testimony from sales and marketing employees, all of whom reside in California. Harris Decl. ¶ 16. Transferring this case to the Northern District of California will save litigation costs and avoid inconveniencing witnesses by forcing them to travel cross-country to this District for trial.

This Court reached a similar conclusion in *Everlast*. There, even though the plaintiff was a New York corporation with offices in New York, 928 F. Supp. 2d at 737–38, the convenience of witnesses, convenience of parties, locus of operative facts, availability of compulsory process, relative means of the parties, and interests of justice "overwhelmingly" favored transfer. *Id.* at 743. The Court gave weight to the convenience of the witnesses identified by the defendants as likely testifying to "germane" topics. *Id.* at 744. Neither the plaintiff's choice of New York (its home forum), the fact that the contracts at issue were executed in New York, nor the fact that New York law governed the contracts at issue overcame the witness convenience factors favoring transfer. *Id*. at 743, 746. This case bears even less relationship to New York, where neither the parties nor facts have significant connections to New York.

Enigma will likely point to its allegations "upon information and belief" that Malwarebytes is detecting ESG's software as PUPs on the computers of ESG customers in New York. FAC ¶ 40. However, testimony regarding their individual experiences is not pertinent to determining *Malwarebytes*' reason for revising and implementing new PUP criteria. In any event, at least 90% of the purported customers that Plaintiff could call as witnesses are *not* known to reside in New York. *See* FAC ¶ 123. Plaintiff thus cannot say that New York is a more convenient forum for customers it might call as witnesses.

2. The Convenience of the Parties Supports Transfer.

Neither party resides in New York. Both parties would thus incur substantial litigation-related inconveniences and costs, including transportation and logistics, if this case is heard in New York. Moreover, transfer would not shift inconveniences from one party to another. In contrast, transfer to California will greatly reduce Malwarebytes' inconveniences and costs.

3. The Location of Evidence Favors Transfer.

Malwarebytes maintains relevant evidence, including documents and data, at its Santa Clara, California headquarters. Harris Decl. ¶ 4. Electronic records created in the course of its business are on servers located in California. *Id*.

4. The Locus of Operative Facts is California.

The core factual issue that Plaintiff alleges is the basis for Malwarebytes' updated PUP criteria. FAC ¶¶ 8, 21. Malwarebytes developed those criteria primarily in California. Harris Decl. ¶ 13. This "primary factor" supports transfer, since transferring to the district "where the key operative events occurred serves 'the interests of justice.'" *Everlast*, 928 F. Supp. 2d at 745 (citations omitted). Moreover, the factor "substantially favors transfer from this district when a party 'has not shown that any of the operative facts arose in the Southern District of New York.'" *SBAV LP*, 2013 WL 3467030, at *4 (citation omitted).

C. <u>The Remaining Factors Are Neutral and Do Not Disfavor Transfer.</u>

The remaining factors do not outweigh the factors favoring transfer. First, while the parties will both incur costs to litigate this matter here, there is no apparent disparity in relative means of the corporate parties. Additionally, there are no complex issues of state law presented; both this Court and the transferee court can apply the law of contract, unfair competition, and tortious interference. *See Everlast*, 928 F. Supp. 2d at 747 (citations omitted) (finding plaintiff could not persuasively argue that there were such "nuanced issues of New York state law" that

the transferor court was "materially more qualified" than the transferee court). Plaintiff's choice of this forum is not entitled to significant deference, given its lack of connection to the District, and the District's lack of connection to the facts of this case. In addition, there are no trial efficiencies to be gained by maintaining the suit in this District. The median times to trial and to disposition in both districts are comparable. *See* United States District Courts-National Judicial Caseload Profile (June 30, 2016), *available at* http://www.uscourts.gov/statistics/table/na/federal-court-management-statistics/2016/06/30-1.

Plaintiff will likely argue that its suit against Bleeping in this District weighs against transfer. It does not when compared to the heavy weighting of all other Section 1404 factors in favor of the Northern District of California. The legal claims against Bleeping and Malwarebytes and issues are distinct, which Plaintiff recognized by filing separate cases instead of joining Malwarebytes in the *Bleeping Computer* case, which predominantly concerns libel. *Bleeping Computer*, Dkt. 25 at 20–21. Plaintiff's claims against Bleeping arise out of a user posting certain content to its website over one year ago, whereas Plaintiff's claims against Malwarebytes arise out of the PUP criteria that Malwarebytes revised for its software in October 2016. Accordingly, the witnesses and evidence in each case will be different, so keeping the cases together would not be more efficient. Moreover, the *Bleeping Computer* case, filed nine months earlier, is at a much different posture. The end of fact discovery in that case is next month, whereas this case is not yet past the pleading stage.

The balance of factors under Section 1404 strongly supports transfer to the Northern District of California for the convenience of witnesses and the interests of justice.

III. THIS COURT LACKS PERSONAL JURISDICTION OVER MALWAREBYTES

A. Malwarebytes Is Not Subject to General Jurisdiction in New York.

Malwarebytes is not incorporated in New York, and its principal place of business is in

California. FAC ¶ 36; Harris Decl. ¶ 5, Ex. A. Plaintiff pled no "exceptional circumstances" demonstrating that Malwarebytes is "essentially at home" in New York and is thus subject to general jurisdiction here. Its unexceptional contacts with New York fall far short of that required to be subject to general jurisdiction here. *See Daimler*, 134 S. Ct. at 762 n.20 ("A corporation that operates in many places can scarcely be deemed at home in all of them.").

B. Malwarebytes Is Not Subject to Specific Jurisdiction.

Plaintiff appears to allege personal jurisdiction under subsections (1), (2), and (3) of CPLR section 302(a) because Malwarebytes "regularly transacts business" in New York, "has committed tortious acts in [the state]," and has "misled and deceived consumers in New York and this District and [] disrupted and disabled their use of ESG's programs . . . ." *See* FAC ¶ 42. The Court lacks specific jurisdiction under any part of CPLR section 302(a).

Malwarebytes did not purposefully direct its alleged activity towards New York. Under subsection 302(a)(1), the court "looks to: (1) whether a defendant has transacted business in such a way that it constitutes purposeful activity; and (2) whether there is an articulable nexus, or a substantial relationship, between the claim asserted and the actions that occurred in New York." *Megna v. Biocomp Labs. Inc.*, 166 F. Supp. 3d 493, 497–98 (S.D.N.Y. 2016). Maintenance of an "interactive" website that is available to, but does not "specifically target," New York users does not establish jurisdiction under section 302(a)(1). *Seldon v. Direct Response Techs., Inc.*, No. 03-5381, 2004 WL 691222, at *5 (S.D.N.Y. Mar. 31, 2004). Plaintiff does not allege facts showing that Malwarebytes' website specifically targeted New York residents.

Instead, Plaintiff relies on the alleged existence of some users of Malwarebytes software in New York. But the Supreme Court held that specific jurisdiction must be based on "contacts that the 'defendant *himself*' creates with the forum State." *Walden v. Fiore*, 134 S. Ct. 1115, 1122 (2014) (citation omitted) (emphasis in original). The Court explained that it has

"consistently rejected attempts to satisfy the defendant-focused 'minimum contacts' inquiry by demonstrating contacts between the plaintiff (or third parties) and the forum State." *Id.* (citations omitted). The Second Circuit has reiterated courts must focus on "the relationship among the defendant, the forum, and the litigation," rather than a plaintiff's or third party's contacts with the forum. *Waldman v. Palestine Liberation Org.*, 835 F.3d 317, 335-37 (2d Cir. 2016). The Court looks to "defendants' suit-related conduct," or "conduct that could have subjected them to liability," to evaluate whether the defendant *itself* created ties with the forum. *Id.* The defendant's conduct is not "sufficiently connected" to the forum state when its liability does not arise from its actions in the forum state. *Id.*

Malwarebytes' "suit-related conduct" occurred in California, where it developed and executed its criteria for PUPs. Harris Decl. ¶ 13. Malwarebytes maintains its website from which its software is distributed in California. *Id*. This software is accessible throughout the United States, and Malwarebytes did not direct its conduct toward New York. *Id.* ¶ 6. Plaintiff's allegation "upon information and belief" that 20 users of both parties' programs happen to reside in New York is insufficient to establish jurisdiction. *See Walden*, 134 S. Ct. at 1123 ("Due process requires that a defendant be haled into court in a forum State based on his own affiliation with the State, not based on the 'random, fortuitous, or attenuated' contacts he makes by interacting with other persons affiliated with the State.").

As to section 302(a)(2), the Second Circuit has held that for non-residents to be subject to New York jurisdiction, "the defendant must commit the tort while he or she is physically in New York State." *Rates Tech.*, 15 F. Supp. 3d at 418 (quoting *Bensusan Restaurant Corp. v. King*, 126 F.3d 25, 28 (2d Cir. 1997) and *Carlson v. Cuevas*, 932 F. Supp. 76, 80 (S.D.N.Y. 1996)). In *Megna*, the court found that a non-resident that operated a website accessible to New York

computer users was "not physically present in New York" on that basis. *Megna*, 166 F. Supp. 3d at 499. Likewise, Malwarebytes has no physical presence in New York relating to its consumer software or PUP criteria changes at issue here. *See* Harris Decl. ¶¶ 5, 10, 11, 13, 15.

Finally, Plaintiff fails to establish jurisdiction under subsection 302(a)(3). To do so, Plaintiff must demonstrate that "'(1) the defendant committed a tortious act outside New York; (2) the cause of action arose from that act; (3) the tortious act caused an injury to a person or property in New York; (4) the defendant expected or should reasonably have expected the act to have consequences in New York; and (5) the defendant derived substantial revenue from interstate or international commerce.'" *Waggaman v. Arauzo*, 117 A.D.3d 724, 725 (N.Y. Ct. App. 2014). Plaintiff summarily concludes that Malwarebytes "misled and deceived consumers in New York" and "disrupted and disabled their use of ESG's programs." FAC ¶ 42. Plaintiff does not, however, plead facts demonstrating that an injury occurred within New York as subsection 302(a)(3) requires. Instead, the FAC shows that users of Plaintiff's programs were notified that the programs were "potentially" unwanted and that the users could decide to continue using the programs. *See, e.g.*, *id.* ¶¶ 32, 86, 90, 93, 102, 113. Even assuming Plaintiff had properly pled injury within the state, subjecting Malwarebytes to personal jurisdiction based merely on injury to a third-party in New York would violate due process. *Walden*, 134 S. Ct. at 1125 ("The proper question is not where the plaintiff experienced a particular injury or effect but whether the defendant's conduct connects him to the forum in a meaningful way"); *see Waggaman*, 117 A.D.3d at 726 (defendant's provision of medical services to a New York resident's mother was "attenuated connection" to forum under *Walden*).

For the above reasons, this Court lacks personal jurisdiction over Malwarebytes, and the FAC should be dismissed with prejudice.

IV. ENIGMA FAILS TO STATE A CLAIM AGAINST MALWAREBYTES

A. Malwarebytes Is Immune From Plaintiff's Claims Under CDA § 230(c)(2).

1. Malwarebytes' PUP Criteria Are Actions to Restrict Access to Objectionable Materials.

As a provider of security software designed to help users block objectionable material such as malware, adware and PUPs, Malwarebytes is immune from Enigma's claims under 47 U.S.C. § 230(c)(2). That section provides statutory immunity to providers of filtering software for good faith blocking and screening of material that the security software providers or their users consider offensive. *Zango*, 568 F.3d at 1173. Specifically, Section 230(c)(2) provides:

> No provider or user of an interactive computer service[4] shall be liable on account of
>
> (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
> (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1) [sic].[5]

Congress enacted the CDA "to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet," 47 U.S.C. § 230(b)(3), and to encourage "development and utilization of blocking and filtering technologies." § 230(b)(4). Courts have consistently held that Section 230 provides "robust" immunity, *Carafano v. Metrosplash.com, Inc.*, 339 F.3d 1119, 1123 (9th Cir. 2003), and that doubts "must be resolved in favor of immunity." *Fair Housing Council v.*

---

[4] "Interactive computer service' means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions." 47 U.S.C. § 230(f)(2).

[5] This CDA provision is different from Section 230(c)(1), which has been asserted by Bleeping Computer. That section provides that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." Enigma sought to hold Bleeping Computer liable as a publisher; Bleeping Computer did not seek immunity under Section 230(c)(2). [Dkt. No. 45]

Roommates.com, LLC, 521 F.3d 1157, 1174 (9th Cir. 2008).

Section 230(c)(2) gives providers of filtering software nearly complete discretion in determining what is objectionable and subject to screening. "[T]he statute plainly immunizes from suit a provider of interactive computer services that makes available software that filters or screens material that the user *or the provider* deems objectionable." *Zango*, 568 F.3d at 1173. Section 230(c)(2)(A) does not require the filtering technology provider to demonstrate that "objectionable" material is actually objectionable. *Zango, Inc. v. Kaspersky Lab, Inc*, No. 07-0807, 2007 WL 5189857, at *4 (W.D. Wash. Aug. 28, 2007). The only restriction on the provider's discretion is that it act in good faith. § 230(c)(2)(A). A plaintiff asserting a claim against a provider of filtering software bears the burden of proving that a provider failed to act in good faith and must plead sufficient facts alleging an absence of good faith to proceed past the pleading stage. *See, e.g.*, *e360 Insight, LLC v. Comcast Corp.*, 546 F. Supp. 2d 605, 608–609 (N.D. Ill. 2008) (ISP's blocking of all of plaintiff's emails to ISP's subscribers was immune from suit under Section 230(c)(2)). Plaintiff has failed to meet that burden.

Zango is the seminal case interpreting Section 230(c)(2), and its facts closely mirror Enigma's factual allegations. The defendant there distributed anti-virus software designed to filter and block potentially malicious software. *Zango*, 568 F.3d at 1171. Defendant's software classified Zango's programs as "adware, a type of malware." Much like Enigma, Zango sued for interference with contractual rights, violation of the Washington Consumer Protection Act, trade libel, and unjust enrichment. *Id.* at 1171–72. Affirming the district court's dismissal of Zango's complaint, the Ninth Circuit held that the defendant was immune under Section 230(c)(2) because its software "enable[d] and [made] available the technical means to restrict access to malware." *Id*. at 1176; *see also e360 Insight*, 546 F. Supp. 2d at 609; *Holomaxx Techs. v.*

Microsoft Corp., 783 F. Supp. 2d 1097, 1104, (N.D. Cal. 2011) (dismissing claims against ISP for blocking plaintiff's emails to subscribers on the basis of Section 230(c)(2) immunity).

Malwarebytes' software is squarely within the scope of the CDA's purpose to "maximize user control" over the computer resources they use. *See* 47 U.S.C. § 230(b)(3). Just like the security software in *Zango*, and the filtering in *Holomaxx* and *e360 Insight*, Malwarebytes' software "filters or screens material that the user or the provider deems objectionable." *Zango*, 568 F.3d at 1173. This screening gives users even greater control than the software in *Zango*, which did not allow users to continue using the blocked programs. *See id.* at 1171. Since the disposition of PUPs is ultimately controlled by Malwarebytes users—who chose to use Malwarebytes in the first place—its screening of PUPs is entirely a good-faith effort to allow users to consider whether the PUPs are "objectionable" as Section 230(c)(2) contemplates.

2. Plaintiff Has Not Sufficiently Pled Absence of Good Faith.

Plaintiff tries to avoid dismissal by scattering conclusory allegations throughout the FAC that Malwarebytes revised its PUP criteria in "bad faith." FAC ¶¶ 1, 8, 21, 76, 126. None of these allegations create a plausible inference of bad faith. *See Holomaxx*, 783 F. Supp. 2d at 1105 (finding alleged profit motive and faulty filtering technology did not show bad faith).

First, the chronology of events renders Plaintiff's allegation that Malwarebytes changed its criteria in response to Plaintiff's lawsuit against Bleeping in January 2016 implausible. Malwarebytes updated its PUP criteria, one of many continual updates, approximately *nine months* after Plaintiff sued Bleeping. FAC ¶¶ 61, 80. That long period flatly contradicts Plaintiff's theory that Malwarebytes' update of its PUP criteria was a retaliatory move, in bad faith. Moreover, Plaintiff does not refute that its software meets one or more of those criteria, or that those criteria are not proper measures of PUPs.

Second, Plaintiff's allegation that Malwarebytes began identifying its programs as PUPs

to gain a competitive advantage is devoid of factual support. If it were plausible that competition motivated Malwarebytes' changes to its PUP criteria, then Malwarebytes would have made those changes not last month, but long ago during the seven years that Malwarebytes and SpyHunter have coexisted—and according to Plaintiff, directly competed—in the market. FAC ¶¶ 6, 71. Further, Malwarebytes' PUP criteria still allow its users to use Plaintiff's programs, behavior that runs contrary to gaining a competitive advantage. *Id.* ¶¶ 10, 86, 90, 93. In all events, Plaintiff has not pled any facts suggesting that the companies actually compete with one another. To the contrary, SpyHunter requires users to purchase a subscription before the product will remove items that it identifies as malicious during its so-called "free scan." FAC ¶¶ 48-49. Consumers use Malwarebytes' core product at no charge.[6] *Id.* ¶ 59.

Allowing Enigma to sidestep CDA immunity at the pleading stage by merely incanting that Malwarebytes has acted in "bad faith" would chill the distribution of consumer-protective filtering technologies and defeat Congress' express intent to encourage the development of filtering technologies and maximize user control over the content to which they are exposed. 47 U.S.C. § 230(b)(3), (4). Faced with the prospect of costly litigation, security vendors are likely to allow aggressive and well-funded PUP vendors that threaten lawsuits to pass through their filters. Enigma is well aware of this and has pursued an intimidation campaign for more than a decade of threatening and filing lawsuits against security companies that have included SpyHunter in their filters. *See* RJN Exs. A-D. While this campaign has no doubt benefited Enigma, it has had the effect of suppressing filtering technologies and reducing consumer control. Indeed, if malware or PUP developers masquerading as "security" companies can always avoid early dismissal of claims against filtering technology providers by alleging anti-competitive intent,

[6] Plaintiff does not allege that Malwarebytes distributes any products that compete with its RegHunter product, which Plaintiff describes as a "registry cleaner." FAC ¶ 47.

then it is logical to expect a growth in distribution of fake, deceptive or malicious security software. The Court should avoid that perverse result here and dismiss Plaintiff's claims.

3. Plaintiff's Lanham Act Claim Does Not Escape Immunity.

All of Enigma's causes of action arise from the same allegations about Malwarebytes' PUP criteria. FAC ¶¶ 7, 139–40, 146, 157, 164. Among other things, Enigma alleges that Malwarebytes "began detecting SpyHunter and RegHunter as PUPs." *Id.* ¶ 81. Since all of Enigma's claims arise from the same effort by Malwarebytes to "enable or make available . . . the technical means to restrict access" to potentially objectionable material, Section 230(c)(2) shields Malwarebytes from liability from all of Enigma's claims. *See Zango*, 568 F.3d at 1173.

Section 230(e)(2), which states that "[n]othing in this section shall be construed to limit or expand any law pertaining to intellectual property," does not apply here. The Lanham Act has two distinct parts: the intellectual property provision, 15 U.S.C. §§ 1114, which concerns infringement of registered trademarks; and the unfair competition provision (Section 43(a)), 15 U.S.C. § 1125(a). Plaintiff alleges violation of only the unfair competition provision of the Lanham Act, and not the trademark infringement provisions. Accordingly, Section 230(c)(2) immunity applies with equal force against Plaintiff's "Lanham Act" claim.

B. Plaintiff Fails to State a Claim Under Section 43(a) of the Lanham Act and New York General Business Law Section 349.

Plaintiff's allegation "of false and misleading statements about ESG" does not state a claim under 15 U.S.C. § 1125(a)(1)(B) or NY GBL § 349. *See* FAC ¶ 73. To state a claim for violation of Section 1125(a)(1)(B), the plaintiff must allege the defendant made "(1) a false or misleading statement (2) in connection with commercial advertising or promotion that (3) was material, (4) was made in interstate commerce, and (5) damaged or will likely damage the plaintiff." *C=Holdings B.V. v. Asiarim Corp.*, 992 F. Supp. 2d 223, 242 (S.D.N.Y. 2013). Plaintiff

fails to satisfy even the predicate element of a false or misleading statement because Malwarebytes' categorization of Plaintiff's software as "Potentially Unwanted Programs" is an opinion that is not actionable under Section 43(a) of the Lanham Act or New York General Business Law § 349. *See ONY, Inc. v. Cornerstone Therapeutics, Inc.*, 720 F.3d 490, 496-98 (2d Cir. 2013) (statements of opinion are not actionable under the Lanham Act or under NY GBL § 349). That is because statements of opinion that are not capable of being proven false are protected under the First Amendment. *Id.* at 496 (citing *Milkovich v. Lorain Journal Co.*, 497 U.S. 1, 19–20(1990)). Determining whether a statement expresses fact or a non-actionable opinion is a question of law. *See, e.g., Steinhilber v. Alphonse,* 68 N.Y.2d 283, 290 (1985)). When determining whether statements are non-actionable opinion, the Court is to consider:

> (1) whether the specific language in issue has a precise meaning which is readily understood; (2) whether the statements are capable of being proven true or false; and (3) whether either the full context of the communication in which the statement appears or the broader social context and surrounding circumstances are such as to signal . . . readers or listeners that what is being read or heard is likely to be opinion, not fact.

Brian v. Richardson, 87 N.Y.2d 46, 51 (1995). Here, the challenged statements that Enigma's programs are "potentially unwanted" are Malwarebytes' opinions, based on criteria that it has developed and refined. The context in which the statements are given further support that the statements constitute Malwarebytes' opinion. *See* FAC ¶¶ 5, 86 (screenshots showing categorization as "potentially" unwanted), ¶¶ 32, 86, 93 (screenshots showing the user's ability to keep wanted programs), Ex. 12 (listing non-exclusive criteria and advising that "we use our judgment"). The challenged statements are not capable of being proven true or false; the decision on whether the programs are wanted or not is for each Malwarebytes user to make. *See Randa Corp. v. Mulberry Thai Silk, Inc.*, No. 00-04061, 2000 WL 1741680, at *3 (S.D.N.Y. Nov. 27, 2000) (dismissing Section 43(a) claim based on statement predicting possibility).

Malwarebytes' description of Enigma's software as "potentially unwanted" is no more factual than ratings given by Better Business Bureaus ("BBB"), which courts have repeatedly held are non-actionable opinions. *See, e.g., Steinmetz v. Energy Automation Sys., Inc.*, No. 500554/13, 2014 WL 1386954, *15, 16 (N.Y. Sup. Ct. Apr. 7, 2014) (collecting cases). In *Steinmetz*, for example, the court dismissed Section 349 claims against two BBBs on the grounds that *inter alia*, ratings are based on the BBBs' evaluation of objective and subjective criteria and reflect the BBBs' opinion and judgment. *Id.* at *17 (citing *Browne v. AVVO, Inc.*, 525 F. Supp. 2d 1249, 1252-53 (W.D. Wa. 2007)). The same is true here. As alleged in the FAC, Malwarebytes based its "potentially unwanted program" listing opinion on its own criteria. FAC ¶¶ 73–74, Ex. 12; *cf. Seaton v. TripAdvisor LLC*, 728 F.3d 592, 601 (6th Cir. 2013) (rejecting defamation claim since listing plaintiff among country's dirtiest hotels reflected opinion, and defendant's "method of compiling" data to create the ranked list was "inherently subjective [in] nature"); *ZL Techs., Inc. v. Gartner, Inc.*, 709 F. Supp. 2d 789, 797 (N.D. Cal. 2010), *aff'd sub nom. ZL Techs., Inc. v. Gartner Grp., Inc.*, 433 F. App'x 547 (9th Cir. 2011) (low rating of software vendor by analyst was "non-actionable opinion" where rating was based on defendant's unverifiable weighing of criteria and conversations with customers and references). Those statements are not actionable, and Plaintiff's Lanham Act and Section 349 claims should be dismissed.

Plaintiff's Lanham Act claim should also be dismissed because it does not allege Malwarebytes' software's labeling of Enigma's programs as PUPS and "threats" were made in "commercial advertising or promotion." To satisfy that element, the statements must be commercial speech "for the purpose of influencing consumers to buy defendant's goods or services," and disseminated sufficiently to the relevant purchasing public. *Fashion Boutique of Short Hills, Inc. v. Fendi USA, Inc.*, 314 F.3d 48, 56-58 (2d Cir. 2002). Only *existing* users of

Malwarebytes software would see the detection of Enigma's programs as PUPs. Enigma tries to salvage its Lanham Act claim by alleging that that Malwarebytes' free anti-malware and AdwCleaner versions are "marketing tools" for its premium products, because certain features in the free versions expire after a 14 day trial period. FAC ¶¶ 59-60. However, Enigma nowhere alleges that the PUP detection and removal features expire. Nor does Plaintiff limit its claims only to uses of Malwarebytes' software within the 14 day Premium trial period.

C. Enigma Has Not Sufficiently Pled Tortious Interference.

Plaintiff's two tortious interference causes of action also fail because Plaintiff failed to plausibly establish that Malwarebytes acted solely out of malice, or used improper or illegal means that would amount to a crime or independent tort. *See Kirch v. Liberty Media Corp.*, 449 F.3d 388, 400 (2d Cir. 2006) (citation omitted) (plaintiff asserting a tortious interference with prospective economic advantage claim must allege the defendant "acted solely out of malice, or used dishonest, unfair, or improper means"). Malwarebytes updated its PUP criteria approximately nine months after the *Bleeping Computer* lawsuit commenced—and approximately seven years after Plaintiff contends that the companies began directly competing with each other—so even any inference of malice is implausible. Plaintiff cannot plausibly allege that Malwarebytes' October 2016 update of its PUP criteria was anything other than a general update to implement the company's long-term strategy for detecting PUPs that resulted in the filtering of numerous PUPs, including Plaintiff's programs. FAC, Ex. 1; *see Medcalf v. Walsh*, 938 F. Supp. 2d 478, 490 (S.D.N.Y. 2013) (dismissing claim for failing to show that defendant plausibly acted with "sole purpose of inflicting intentional harm" on the plaintiff).

Plaintiff's tortious interference with business relations claim also fails because Plaintiff identifies no prospective customers who experienced interference. *See Parekh v. Cain*, 96 A.D.3d 812, 816 (N.Y. Ct. App. 2012) (dismissing claim "since the complaint did not identify the third

party with whom the plaintiff was engaging in business relations"); *Zetes v. Stephens*, 108 A.D.3d 1014, 1020 (N.Y. Ct. App. 2013). Moreover, because it is undisputed that Malwarebytes' screening software only identifies PUPs as potentially unwanted and instructs the customer to choose whether to continue using each PUP, there is simply no tortious or unlawful activity that could support causes of action for tortious interference.

CONCLUSION

Malwarebytes respectfully requests that the Court transfer this action to the Northern District of California pursuant to 28 U.S.C. § 1404, for the convenience of witnesses and in the interest of justice because almost all of the relevant witnesses and evidence reside in California. Alternatively, Malwarebytes requests dismissal for lack of personal jurisdiction. If the Court determines personal jurisdiction and venue are proper, this Court should dismiss Enigma's lawsuit in its entirety for failure to state any claim against Malwarebytes.

Dated: December 28, 2016

Respectfully submitted,

FENWICK & WEST, LLP

By: *s/ Tyler G. Newby*
Attorneys for Defendant
MALWAREBYTES INC.

Tyler G. Newby (admitted *pro hac vice*)
tnewby@fenwick.com
Sapna Mehta (admitted *pro hac vice*)
smehta@fenwick.com
555 California Street, 12th Floor
San Francisco, CA 94104
Telephone: 415.875.2300
Facsimile:415.281.1350